IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Ralph Samuel HOEFELMEYER et al.	Confirmation No.: 3657
Application No.: 09/911,592	Group Art Unit: 2131
Filed: July 24, 2001	Examiner: CHEN, S.
Attorney Docket: COS00019 Client Docket: 09710_1007	

For: NETWORK SECURITY ARCHITECTURE

REPLY BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Reply Brief is submitted in response to the Examiner's Answer mailed February 22, 2008.

I. STATUS OF THE CLAIMS

Claims 1-15 are pending and are on appeal.

II. GROUNDS OF REJECTION TO BE REVIEWED

Whether claims 1, 3, 5, 8, and 10 are properly provisionally rejected under obviousness-type double patenting over claims 1, 4, 7, 11, and 14 of co-pending Application Serial No. 10/024,202?

Whether claims 1, 3, 5, 6, 8, and 10-15 are obvious under 35 U.S.C § 103 based on *Hypponen et al.* (US 2003/0191957) in view of *Yanovsky* (US 7,010,807)?

Whether claims 2, 4, 7, and 9 are obvious under 35 U.S.C § 103 based on *Hypponen et al.* (US 2003/0191957) and *Yanovsky* (US 7,010,807) in view of *Network Associates, Inc. (NAI)*?

III. ISSUES

1. Whether claims silent as to any security manager and the taking of any action responsive to detection of a malicious code are, *per se*, obvious over claims which recite that, responsive to detection of a malicious code, an even indicating the detection is generated and transmitted to a security manager?
2. Whether the "plurality of intranets" of the claims on appeal is merely a "duplication of parts"?

IV. ARGUMENT

Appellants maintain and rely on the arguments set forth in the principal Appeal Brief of November 29, 2007, which are incorporated herein by reference. Additionally, Appellants provide the following comments with regard to the Examiner's response in the Examiner's Answer:

1. The Examiner again cites *Titanium Metals Corp. v. Banner*, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) for the proposition that an earlier species disclosure in the prior art defeats any generic claim. Appellants must again stress that the *Titanium* case is not applicable to the present situation since we are dealing with an obviousness-type double patenting issue here and not, as in *Titanium*, an anticipation issue. Moreover, genus/species obviousness analyses as advanced by the Examiner are generally less applicable to electrical cases, as in the present case,

than to chemical issues with which *Titanium* was concerned. The Examiner is still clearly asserting that because the instant claims on appeal are broader in scope than the claims of the co-pending application, the present claims **must** be obvious over those of the co-pending application. Appellants stress that while this may be true in some cases, there is no *per se* rule, as the Examiner appears to argue, that makes it **always** true. Each case must be treated on its own merits and, in the instant case, the Examiner has articulated no rationale basis for concluding that it would have been obvious to **not** notify an administrator when a malicious code has been detected in view of a teaching that **always** generates an event indicating detection of a malicious code. The Examiner merely asserts the conclusion of obviousness based on the instant claims being broader than those of the co-pending application, with no accompanying rationale as to why it would have been obvious to delete such notification.

Appellants stress that it is not always obvious, certainly not *per se* obvious, to remove or delete a feature from claimed subject matter. The claims of the co-pending application require that in response to detection of a malicious code, an event is generated and transmitted, that event indicating the detection of the malicious code to a security manager. That is the teaching of the co-pending claims, i.e., that in response to a detection of malicious code, a security manager **must** be notified of the occurrence of such a malicious code. There is no suggestion in those co-pending claims that a network security system deployed between a plurality of intranets and comprising a scanning system for scanning mail for malicious code, an anti-virus server for downloading anti-virus code, and a switch for directing mail from an internet backbone to the scanning system may exist **without** always notifying a security manager of the occurrence of a malicious code.

While it might appear obvious to the Examiner, in hindsight, to merely delete the notification step of the co-pending claims, the Examiner has offered no evidence to substantiate the conclusion of obviousness. In the absence of any such evidence, including some cogent rationale for reaching this conclusion, the Examiner has failed to present a *prima facie* case of obviousness-type double patenting, indicating why it would have been obvious, from a teaching of responsive to the detection of a malicious code, generating and transmitting an event indicating the detection to a security manager, to **not** generate and transmit such an event to a security manager.

Accordingly, this Honorable Board is respectfully requested to reverse the Examiner's provisional rejection of claims 1, 3, 5, 8, and 10 under obviousness-type double patenting over claims 1, 4, 7, 11, and 14 of co-pending Application Serial No. 10/024,202.

2. The Examiner admits that *Hypponen et al.* fails to disclose a plurality of intranets in a network infrastructure, but finds that Appellants' claimed "plurality of intranets" is merely a duplication of parts (intranets) and that there is "no patentable significance" (Examiner's Answer of February 22, 2008-page 10) in this "plurality of intranets" as compared with the single intranet (presumably, network 1) taught by *Hypponen et al.*

With all due respect, Appellants' contribution to the art is more than a "mere duplication of parts." *Hypponen et al.* suggests a centralized virus scanning process which avoids the need to provide virus scanning functionality at each of the individual transit nodes (see paragraph [0011]), but there is absolutely no suggestion in *Hypponen et al.* that the disclosed system may be applicable to a much wider area consisting of multiple intranets connected within a larger network security system. That is, *Hypponen et al.* discloses a computer data network 1

comprising a single physical wire network 3 to which each of a plurality of users is connected. Appellants' claimed invention, on the other hand, provides advantages that *Hypponen et al.* cannot provide. Appellants' network security system is shared between various organizations each having its own intranet. The ability to use a single scanning system and a single anti-virus server to perform inspections for malicious code throughout all of the connected intranets is an important contribution by Appellants that is not disclosed or suggested by *Hypponen et al.* The Examiner's unsupported allegation that it would have been obvious to extend the system of *Hypponen et al.* to include a plurality of intranets, when nothing of the kind is suggested by *Hypponen et al.*, is an exercise of hindsight based on pure speculation. It is not a simple matter to merely take the single network of *Hypponen et al.* and extend that system to provide malicious code detection to a plurality of intranets by providing a single scanning system coupled to the plurality of intranets for scanning incoming electronic mail for malicious code, a single anti-virus server coupled to the plurality of intranets for downloading anti-virus code to clients coupled to the plurality of intranets, and a switch coupled between an internet backbone, the scanning system and the anti-virus server for directing the incoming electronic mail from the internet backbone to the scanning system, and the Examiner provides no cogent rationale that would have led the skilled artisan to make such a modification to *Hypponen et al.*

To whatever extent *Yanovsky* may teach a module for updating anti-virus protection on network devices, there would have been no discernible reason for modifying *Hypponen et al.* with any such module because *Hypponen et al.* is not concerned with detecting viruses or malicious code across a plurality of intranets. Rather, *Hypponen et al.* is concerned with only a single network. Moreover, because of this single network, contrary to the Examiner's position, *Hypponen et al.* would have no need of the claimed "switch coupled between the internet

backbone, the scanning system, and the anti-virus server…for directing incoming electronic mail from the internet backbone to the scanning system," as claimed.

The Examiner's allegation that *Hypponen et al.* "would operate equally with a single intranet or a plurality of intranets" (Examiner's Answer-page 10) is an unsupported conclusion based on speculation as *Hypponen et al.* is not equipped with the necessary anti-virus server needed for downloading anti-virus code to various clients coupled to a plurality of intranets, or with the necessary switch for directing incoming electronic mail from the internet backbone to the scanning system, as claimed, and *Yanovsky* provides no incentive for the skilled artisan to modify *Hypponen et al.* in any manner to achieve the claimed network security system deployed between a plurality of intranets.

V. CONCLUSION AND PRAYER FOR RELIEF

The claims require a network security system to be deployed between a plurality of intranets but neither *Hypponen et al.* nor *Yanovsky* suggests such a plurality of intranets or the inclusion of a switch coupled between the internet backbone, the scanning system, and the anti-virus server, configured to direct incoming electronic mail from the internet backbone to the scanning system. Appellants, therefore, request the Honorable Board to reverse each of the Examiner's rejections.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 504213 and please credit any excess fees to such deposit account.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

April 10, 2008
Date

/Errol A. Krass/
Errol A. Krass
Attorney for Applicant(s)
Reg. No. 60090

Phouphanomketh Ditthavong
Attorney for Applicant(s)
Reg. No. 44658

Customer No.:

25537